SUMÁRIO

1 Objetivo
2 Campo de Aplicação
3 Responsabilidade
4 Documentos Complementares
5 Siglas
6 Considerações Gerais
7 Itens Revisados e Prazo para Implementação
Anexo - OECD Number 10 The Application of The Principles of GLP to Computerised Systems. 1995.

1 OBJETIVO

Esta Norma estabelece requisitos complementares para laboratórios que realizam estudos segundo os Princípios das Boas Práticas de Laboratório – BPL, e deve ser utilizada em complemento à NIT-DICLA 035.

2 CAMPO DE APLICAÇÃO

Este documento aplica-se à Cgcre/Dicla, aos inspetores e aos laboratórios que já atuam ou irão atuar segundo os Princípios das Boas Práticas de Laboratório - BPL.

3 RESPONSABILIDADE

A responsabilidade pela revisão desta Norma é da Dicla .

4 DOCUMENTOS COMPLEMENTARES

OECD	Principles on Good Laboratory Practice (as revised in 16.156.157). OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 1. Paris (França), 16.156.156.14.
DOQ-CGCRE-001	Orientações para a acreditação de laboratórios de calibração e de ensaio.
NIT-DICLA-013	Concessão, manutenção e extensão da acreditação de laboratórios.
NIT-DICLA-030	Rastreabilidade ao Sistema Internacional de Unidades no Credenciamento de Laboratórios
NIT-DICLA-031	Regulamento da acreditação de laboratórios.
NIT DICLA 034	Critérios para a acreditação de laboratórios de ensaios BPL – Boas Práticas de Laboratório – Aplicação a Estudos de Campo

5 SIGLAS

BPL	Boas Práticas de Laboratório
CAS	Chemical Abstract Service
CT	Comissão Técnica
DE	Diretor de Estudo
Dicla	Divisão de Credenciamento de Laboratórios
Cgcre	Coordenação Geral de Acreditação
GIT	Gerente da Instalação de Teste
Inmetro	Instituto Nacional de Metrologia, Normalização e Qualidade Industrial
OECD	Organization for Economic Cooperation and Development
OCDE	Organização de Cooperação e Desenvolvimento Econômico
PE	Plano de Estudo
POP	Procedimento Operacional Padrão
PP	Pesquisador Principal
RF	Relatório Final
GQ	Garantia da Qualidade
IT	Instalação de Teste

6 CONSIDERAÇÕES GERAIS

Os Princípios das Boas Práticas de Laboratórios são aplicados à laboratórios que realizam estudos exigidos por órgãos regulamentadores visando avaliar o risco ambiental e saúde humana dos produtos agrotóxicos, farmacêuticos, aditivos de alimentos e rações, cosméticos, veterinários, químicos industriais, Organismos Geneticamente Modificados-OGM.
Objetivando o reconhecimento mútuo de dados laboratoriais de acordo com BPL, a Cgcre/Inmetro decidiu utilizar a tradução do documento Number 1 da Organization for Economic Cooperation and Development- OECD Principles on Good Laboratory Practice (as revised in 1997). Paris 1998 e o documento complementar Number 10 da Organization for Economic Cooperation and Development- OECD The Application Of The Principles Of GLP To Computerised Systems. 1995, estabelecido nesta NIT-DICLA.

7 PRAZO PARA IMPLEMENTAÇÃO

Esta Norma deve ser implementada a partir de 01 de fevereiro de 2008.

ANEXO
VERSÃO BRASILEIRA DA PUBLICAÇÃO OECD Number 10 "THE APPLICATION OF THE PRINCIPLES OF GLP TO COMPUTERISED SYSTEMS". 1995.

Nota: Por tratar-se de tradução de documento em língua estrangeira, este documento não segue as prescrições da NIG-GQUAL-001.

A APLICAÇÃO DOS PRINCÍPIOS BPL À SISTEMAS INFORMATIZADOS

Introdução

Tem se observado recentemente que a utilização dos sistemas informatizados tem aumentado nas Instalações de Teste que realizam ensaios de segurança para a saúde e o meio ambiente. Estes sistemas informatizados podem permitir, direta ou indiretamente, a aquisição, processamento, apresentação e armazenamento de dados. Estes se encontram, cada vez mais, integrados freqüentemente nos equipamentos automatizados. Quando estes sistemas Informatizados se encontram combinados com a execução de estudos para fins regulatórios, seu conceito, sua validação, sua operação e sua manutenção devem estar em conformidade com os Princípios de Boas Práticas Laboratório.

Campo de aplicação

Todos os sistemas informatizados que são utilizados para produzir, medir ou avaliar os dados com fins regulatórios devem ser desenvolvidos, validados, operados e mantidos de acordo com os Princípios de BPL.

Para o planejamento, execução e apresentação dos resultados dos estudos podem ser utilizados diversos sistemas informatizados. Estes sistemas podem ser aplicados para adquirir, direta ou indiretamente, os dados registrados por meio dos equipamentos automatizados, operar / controlar os equipamentos automatizados e finalmente, processar, apresentar e armazenar os dados. Os sistemas informatizados utilizados para tais atividades podem ser de diversas índoles e podem incluir desde instrumentos de análises programáveis ou um computador pessoal, até um sistema de gestão das informações do laboratório (LIMS-Laboratory Information Management System) de funções múltiplas. Os Princípios de BPL devem ser aplicados sejam quais forem os graus de intervenção do computador ou das pessoas.

Abordagem

Os sistemas informatizados, associados à execução dos estudos com fins regulatórios, devem ser adequadamente projetados, dispor de uma capacidade suficiente e serem convenientes para as tarefas as quais estão destinados. Os procedimentos adequados devem ser escritos para controlar e administrar estes sistemas, que devem estar projetados, validados e serem operados em conformidade com os Princípios de BPL.

Também desempenha um papel determinante a operação denominada "validação", que permite demostrar que um sistema informatizado está adaptado às tarefas para as quais se destina.

O procedimento de validação apresenta as suficientes garantias para poder permitir que um sistema informatizado responda as condições pré estabelecidas. A validação deve corresponder a um plano de validação formal e deverá ser realizada antes de colocar o sistema em operação.

APLICAÇÃO DOS PRINCÍPIOS DE BPL AOS SISTEMAS INFORMATIZADOS

As considerações a seguir devem facilitar a aplicação dos Princípios de BPL aos sistemas informatizados:

1. RESPONSABILIDADES

a) O Gerente da Instalação de Teste (GIT) assume a responsabilidade geral da aplicação dos Princípios de BPL. Fundamentalmente, corresponde a este assegurar um número adequado de pessoas suficientemente qualificadas e com experiência. Organizar eficazmente seu trabalho, assim como zelar para que as instalações, os equipamentos e os procedimentos de gestão de dados correspondam a normas requeridas.

O GIT é responsável por supervisar que os sistemas informatizados estejam de acordo com as tarefas para as quais estão destinados. Assim, deverá definir as instruções e procedimentos para garantir que os sistemas informatizados sejam projetados, validados, operados e mantidos em conformidade com os Princípios de BPL. O GIT também deve assegurar que estas instruções e procedimentos sejam compreendidos e seguidos por todos e assegurar o controle efetivo da aplicação destas disposições.

O GIT deve contratar pessoal encarregado especificamente do desenvolvimento, validação, operação e manutenção dos sistemas informatizados. Este pessoal deverá ter qualificação suficiente e passar por treinamento apropriado, além de ter recebido capacitação adequada para assumir as tarefas que são encarregadas de acordo com o Princípios de BPL.

b) O Diretor de Estudo tem a responsabilidade da aplicação dos Princípios de BPL na condução geral de seus estudos. Considerando que estes estudos devem recorrer freqüentemente aos sistemas informatizados, é indispensável que os Diretores de Estudos estejam perfeitamente familiarizados com a utilização de qualquer sistema informatizado que intervenha nos estudos que estejam sob sua supervisão.

Ao tratar-se dos dados registrados por meios eletrônicos, a responsabilidade do Diretor de Estudo é a mesma que quando se trata dos dados registrados em papel e, desta maneira, somente os sistemas validados poderão ser utilizados em estudos BPL.

c) Todo o pessoal que utiliza sistemas informatizados deverá operar estes sistemas de acordo com os Princípios de BPL. Assim, pessoal encarregado de desenvolver, validar, operar e mantém sistemas informatizados são responsáveis por conduzir essas atividades de acordo com Princípios de BPL e de acordo com normas técnicas reconhecidas.

d) As responsabilidades da Garantia da Qualidade (GQ) dos sistemas informatizados devem ser definidas pelo GIT e descritas em políticas e procedimentos escritos. A Garantia da Qualidade deverá compreender os procedimentos e as práticas que permitam garantir o devido respeito das normas estabelecidas em todas as etapas da validação, operação e manutenção dos sistemas informatizados. Além disto, devem ser estabelecidos procedimentos e práticas para a introdução dos sistemas adquiridos e para a adaptação de sistemas informatizados às necessidades internas.

O pessoal encarregado da Garantia da Qualidade deverá verificar se os sistemas informatizados estão de acordo com as BPL e deverá receber a capacitação técnica especializada que a situação assim exige. Deverá conhecer suficientemente estes sistemas para poder formular comentários objetivos e em certos casos, será conveniente recorrer a auditores especializados em sistemas informatizados.

O pessoal encarregado da GQ deverá ter acesso somente à leitura aos dados armazenados nos sistemas informatizados para seu controle.

2. CAPACITAÇÃO

Como forma de atender aos princípios das BPL, as instalações de testes devem empregar pessoal qualificado e experiente. Devem existir programas de treinamento documentados incluindo treinamentos no local de trabalho e, quando aplicável, cursos externos. Devem ser conservadas as documentações relativas a estas capacitações.
As disposições anteriores devem ser aplicadas a todo o pessoal que se utilizam de sistemas informatizados.

3. INSTALAÇÕES E EQUIPAMENTOS

Deverá dispor de instalações e equipamentos adequados para garantir a correta execução dos estudos, sempre em conformidade com os princípios de BPL. Ao tratar-se dos sistemas informatizados, devem ser considerados alguns aspectos específicos:

a) Instalações

Deve haver um estudo detalhado da localização dos equipamentos, dos elementos periféricos, dos equipamentos de comunicação e dos sistemas eletrônicos de armazenamento. Deve se evitar as fortes variações de temperatura e de umidade, o pó, as interferências eletromagnéticas e a proximidade de cabos de alta tensão, exceto se o equipamento estiver especialmente projetado para funcionar em tais condições.

Também deve ser estudada a alimentação elétrica dos equipamentos informatizados, e quando apropriado, uma alimentação de emergência e sem interrupções para os sistemas informatizados cuja interrupção repentina poderia alterar os resultados de um estudo.
Também devem ser considerados os equipamentos adequados para garantir a segurança do suporte eletrônico de informações.

b) Equipamento

Hardware e software
Um sistema informatizado constitui de um grupo de *hardware* e *software,* projetados e preparados para executar uma função ou um grupo de funções determinadas.

O *hardware* constitui a parte física do sistema informatizado e é formado pela unidade central do computador e seus periféricos.

O *software* corresponde ao(s) programa(s) necessário(s) para a operação do sistema informatizado. Todos os Princípios de BPL aplicáveis aos equipamentos também têm aplicação ao *hardware* e ao *software*.

Comunicações

As comunicações associadas aos sistemas informatizados correspondem, em seu sentido mais amplo, a duas categorias: a comunicação que vários computadores podem ter entre si ou a comunicação entre computadores e seus sistemas periféricos.

Todos os sistemas de intercomunicação podem constituir fontes potenciais de erro e podem acarretar a perda ou a alteração dos dados. Devem ser consideradas as medidas de controle adequadas para garantir a segurança e a integridade dos sistemas no momento do desenho, da validação, da operação e da manutenção de qualquer sistema informatizado.

4. MANUTENÇÃO E RECUPERAÇÃO DE ACIDENTE

Todos os sistemas informatizados devem ser instalados e mantidos com o objetivo de garantir um correto funcionamento de forma contínua.

a) Manutenção

Deve haver procedimentos estabelecidos por escrito que descrevam a manutenção rotineira e não rotineira. Estes procedimentos devem definir claramente as funções e as responsabilidades do pessoal envolvido. Quando estas atividades de manutenção causarem a modificação do hardware e/ou do software, poderá ser necessário validar de novo o sistema. Todos os problemas e anomalias detectados durante a operação do sistema, assim como as medidas corretivas aplicadas, devem ser registradas por escrito.

b) Recuperação de acidente

Será preciso dispor de procedimentos que descrevam as medidas que devem ser tomadas no caso de uma falha parcial ou completa de um sistema informatizado. Estas medidas podem no começo ser redundantes para certos equipamentos e, finalizar retornando ao sistema com o suporte de papel.
Todos os planos de emergência devem estar suficientemente detalhados e validados, garantir a integridade permanente dos dados e não comprometer de nenhum modo a execução do estudo. O pessoal que participa nos estudos, em conformidade com os Princípios de BPL, deve estar devidamente informado de todos estes planos de emergência.
Os procedimentos de recuperação do processamento de um sistema informatizado dependerão sempre da importância do sistema, entretanto, é indispensável conservar cópias de segurança de todos os softwares. Caso os procedimentos de recuperação precisem de uma modificação do hardware ou do software, poderá ser necessário validar de novo o sistema.

5. DADOS

Os Princípios de BPL definem os dados brutos como um conjunto de registros e documentos originais do laboratório, inclusive os dados incorporados diretamente em um computador por mediação de uma interface de instrumentação, que se deriva por sua vez das observações e das atividades originais de um estudo e, que são necessários para a reconstituição e avaliação do relatório final deste estudo.

Os sistemas informatizados operados em conformidade com os Princípios de BPL, podem estar associados a dados brutos de diversos tipos como por exemplo: mídia de dados eletrônicos, de saídas de computadores ou de instrumentos, incluindo microfilmes/fichas. Os dados brutos devem ser definidos para cada sistema informatizado.

Sistemas informatizados utilizados para adquirir, processar, relatar ou armazenar eletronicamente os dados brutos devem estar sempre projetados para que exista a possibilidade de proceder a uma análise retrospectiva para que apareçam todas as modificações dos dados sem ocultar os dados iniciais. Também deverá ser possível associar a cada modificação à pessoa que realizou a alteração, por meio de assinaturas (eletrônicas) com incorporação de data e hora. As modificações devem ser justificadas em todos os casos.

Quando os dados brutos são conservados em meios eletrônicos, será preciso garantir as condições necessárias para a conservação ao longo prazo do tipo de dados correspondentes, considerando a duração útil dos sistemas informatizados. Em caso de modificação de *hardware* e de *software*, deverá existir sempre a possibilidade de se acessar e conservar os dados brutos sem correr o risco de comprometer sua integridade.

As informações auxiliares, basicamente os registros de manutenção/calibração, necessários para verificar a validade dos dados brutos ou permitir a reconstituição de um processo ou de um estudo, devem ser sempre arquivados devidamente.

Os procedimentos de operação de um sistema informatizado devem também descrever os procedimentos de aquisição de dados de substituição que serão utilizados em caso de falha do sistema. Neste caso, todos os dados brutos registrados manualmente após serem adquiridos, devem ser claramente identificados como tais e conservados com o título de registros originais. Os procedimentos manuais de segurança podem servir para reduzir os riscos de perda de dados e dar a segurança de que os registros de substituição serão devidamente conservados.

Quando um sistema se tornar obsoleto e for necessário transferir os dados brutos para outro sistema eletronicamente, deve ser utilizado procedimento devidamente seguro cuja integridade seja verificada previamente. Caso não se possa proceder com esta transferência, os dados brutos devem ser transferidos por outro meio e deve ser verificada a exatidão da cópia antes de destruir os arquivos eletrônicos originais.

6. SEGURANÇA

Deve haver procedimentos de segurança suficientemente seguros para proteger o *hardware*, o *software* e os dados contra qualquer alteração, modificação não autorizada ou perda. Neste contexto, a segurança abrange também a prevenção do acesso não autorizado ou as modificações do sistema informatizado e dos dados contidos no sistema. Também será conveniente considerar os riscos de alteração dos dados por vírus ou outros fenômenos. Também deve-se tomar as medidas de segurança necessárias para garantir a integridade dos dados no caso de falha do sistema a curto ou longo prazo.

Segurança física

Devem ser consideradas as medidas físicas de segurança para limitar somente ao pessoal autorizado o acesso aos equipamentos informatizados, aos equipamentos de comunicação, aos periféricos e aos suportes eletrônicos. Tratando-se dos equipamentos que não se encontram instalados em salas dedicadas (computadores pessoais e terminais, por exemplo), será preciso ter no mínimo, um controle convencional para o acesso à Unidade Operacional. No entanto, quando estes equipamentos se encontrarem situados a distância (elementos portais ou ligados por placa de modem) devem ser tomadas outras medidas correspondentes ao caso.

Segurança lógica (*software*)

Para cada sistema ou aplicativos de caráter informatizado, devem ser tomadas as medidas de segurança lógica para impedir o acesso não autorizado aos sistemas, aplicativos e dados informatizados. É indispensável garantir que somente devem ser utilizadas as versões aprovadas e os softwares validados. Segurança lógica pode incluir o uso de uma identidade única para cada usuário, acompanhada de uma contra-senha. Qualquer introdução de dados ou de *softwares* procedentes de fontes externas deverá estar devidamente controlada. Estes controles podem ser obtidos por meio do software de operação, por programas específicos de segurança, programas integrados as aplicações ou por vários destes meios em combinação.

Integridade dos dados

Considerando que a manutenção da integridade dos dados constitui um dos objetivos preliminares dos princípios de BPL, é preciso que qualquer pessoa envolvida em um sistema informatizado saiba que é indispensável considerar as diversas proposições que acabam de ser mencionadas em matéria de segurança.

O gerente deve estar seguro de que o pessoal é perfeitamente consciente da importância da segurança dos dados e que conheçam os procedimentos e funções do sistema que permitem garantir uma correta segurança, assim como as conseqüências de qualquer defeito de segurança. Estas funções podem corresponder a uma vigilância de rotina do acesso ao sistema, a aplicação de programas de verificação dos arquivos e a notificação de anomalias e/ou tendências.

Back up

Na prática, quando se utilizam sistemas informatizados, é comum fazer back up de todos os *softwares* e dados para poder reiniciar o sistema caso haja uma falha que comprometa a integridade do mesmo (deterioração do disco rígido, por exemplo). Consequentemente a cópia de segurança deve constituir uma fonte de dados brutos que serão processados como tais.

7. VALIDAÇÃO DOS SISTEMAS INFORMATIZADOS

Os sistemas informatizados devem estar adaptados às tarefas para as quais estão destinados. Devem ser considerados os seguintes aspectos:

Aceitação

Os sistemas informatizados devem estar projetados em conformidade com os princípios de BPL e sua introdução deve ser planejada previamente em todos os casos. Uma documentação adequada deve demonstrar que cada sistema foi desenvolvido sob controle e, de preferência, em conformidade com normas de qualidade e com normas técnicas reconhecidas (ISO 9001, por exemplo). Além disto, parece importante dispor de elementos concretos que demonstrem que a conformidade do sistema com os critérios de aceitação foram validados antes do sistema ser colocado em serviço. Os testes oficiais de aceitação devem ser realizados seguindo um plano previamente determinado e devem conservar os documentos relativos a todos os procedimentos, dados e resultados, bem como um resumo preciso destes testes e um documento oficial de recepção. No caso de sistemas fornecidos por um vendedor, uma grande parte da documentação criada durante o decorrer do desenvolvimento permanecerá em certos casos em poder do vendedor. Em tais casos, deverá se conservar na Unidade Operacional um dossiê relativo a avaliação e/ou verificação oficial pelo vendedor.

Avaliação retrospectiva

Para certos sistemas, pode ocorrer que a necessidade de conformidade com os princípios de BPL não tenha sido prevista nem especificada. Em tal caso, será conveniente dispor de elementos que permitam justificar a utilização destes sistemas. Basicamente, se tratará de uma avaliação retrospectiva para avaliar esta adequação.

Uma avaliação retrospectiva inicia-se pela coleta de todas as informações retrospectivas relativas ao sistema informatizado. Estes registros devem ser examinados e um resumo escrito deve ser preparado. Este resumo de avaliação retrospectiva deverá indicar os elementos disponíveis que apoiam uma validação e como será preciso proceder no futuro para que o sistema informatizado seja validado.

Controle das modificações

O controle das modificações constitui a aprovação e a justificativa oficial, documentos de apoio, de qualquer modificação do sistema informatizado durante a operação do mesmo. O controle das modificações será necessária quando uma modificação correr o risco de atingir a validade do sistema informatizado. Os procedimentos de verificação das modificações devem estar efetivos a partir do momento em que o sistema passa a ser operado.

O procedimento deverá descrever o método de avaliação para determinar qual a extensão dos testes necessários para manter a validade do sistema. Os procedimentos de verificação das modificações devem descrever os nomes das pessoas responsáveis em determinar se uma verificação das modificações é necessária e, em caso afirmativo, aprová-la.

Seja qual for a origem da modificação (provedor ou desenvolvimento interno), uma informação adequada deverá estar disponível no marco do processo de verificação das modificações. Os procedimentos de verificação devem garantir a integridade dos dados.

Mecanismo auxiliar

Para ter segurança de que um sistema informatizado continua adaptado às tarefas para as quais está destinado, devem existir mecanismos auxiliares para garantir o funcionamento e o uso correto do sistema. Pode haver disposições relativas à administração do sistema, capacitação, manutenção, assistência técnica, auditoria e/ou avaliação dos resultados obtidos. A avaliação dos resultados obtidos consiste em um exame oficial efetuado periodicamente, com o objetivo de verificar que o sistema continua respondendo sempre aos critérios de resultados práticos, em termos, basicamente de confiabilidade, sensibilidade e de capacidade.

8. DOCUMENTAÇÃO

Os elementos descritos a seguir têm por objeto descrever, a título informativo, a documentação mínima necessária para o desenvolvimento, validação, operação e manutenção dos sistemas informatizados.

Políticas

Devem existir políticas escritas da gerência, que incluam basicamente, a aquisição, características, conceito, validação, experimentos, instalação, operação, manutenção, pessoal responsável, controle, auditoria e verificação dos sistemas informatizados.

Descrição ~~das~~ dos aplicativos

Para cada aplicativo, deve-se dispor de uma documentação completa relativa a:

- A denominação do software de aplicação ou o código de identificação, assim como uma descrição clara e detalhada do objetivo do aplicativo.
- O hardware (com os números dos modelos) sobre o qual se opera o software aplicativo.
- O sistema operacional e os demais softwares (ferramentas, por exemplo) utilizados em relação ao aplicativo.
- A(s) linguagem(ns) de programação de aplicação e/ou as ferramentas de bases de dados que se utilizam.
- As principais funções executadas pelo aplicativo.
- Uma descrição geral dos tipos e fluxos de dados do conceito das bases de dados associadas ao aplicativo.
- As estruturas dos arquivos, as mensagens de erro, alarme e os algoritmos associados ao aplicativo.
- Os módulos do software aplicativo com os números de versões.
- A configuração e as interfaces entre os módulos aplicativos e os equipamentos / outros sistemas.

Código de fonte

É recomendável que o código de fonte do software de aplicação esteja acessível ou possa ser obtido na instalação de teste.

Procedimentos Operacionais Padrão

Uma grande parte da documentação relativa a utilização dos sistemas informatizados, deve estar na forma de Procedimentos Operacionais Padrão. Entre outros devem incluir:

- Os procedimentos relativos à operação dos sistemas informatizados (*hardware / software*) e as responsabilidades do pessoal envolvido.
- Os procedimentos relativos às medidas de segurança utilizadas para detectar e prevenir-se contra os acessos não autorizados e as modificações dos programas.
- Os procedimentos e autorizações relativas às modificações dos programas e registros das modificações.
- Os procedimentos e autorizações relativos às modificações dos equipamentos (*hardware* / *software*), e inclusive, dependendo o caso, os teses antes da utilização.
- Os procedimentos relativos aos testes periódicos para verificar o funcionamento da totalidade do sistema ou de certos elementos, e o registro destes testes.
- Os procedimentos relativos a manutenção dos sistemas informatizados e de qualquer outro equipamento auxiliar.
- Os procedimentos relativos ao desenvolvimento de softwares e os testes de recepção, assim como o registro de todos os testes de recepção.
- Os procedimentos de backup para todos os dados armazenados e os planos de emergência em caso de falhas.
- Os procedimentos relativos aos arquivos e a extração de todos os documentos, softwares e dados informatizados.
- Os procedimentos relativos ao controle e a verificação dos sistemas informatizados.

9. ARQUIVOS

Os princípios de BPL relativos aos arquivos dos dados devem ser aplicados sistematicamente para todos os tipos de dados. Consequentemente, é de suma importância que os dados informatizados se encontrem armazenados com os mesmos níveis de controle de acesso, de indicação e de facilidade de recuperação que os demais tipos de dados.

Quando os dados eletrônicos de mais de dois estudos forem armazenados em um único meio (disco rígido ou fita), deve se existir um índice detalhado.

Também poderá ser necessário adotar instalações com controles ambientais apropriados para garantir a integridade dos dados informatizados armazenados. Caso seja necessária a instalação adicional de arquivos, a gerência deve definir o pessoal responsável pela gestão dos arquivos e limitar o acesso somente ao pessoal autorizado.

Também será preciso implementar procedimentos para garantir a integridade a longo prazo dos dados armazenados eletronicamente. Caso o acesso aos dados a longo prazo possam causar problemas ou se existe a possibilidade dos sistemas informatizados ficarem fora de serviço, devem ser estabelecidos procedimentos adequados para garantir que os dados continuem sendo legíveis. Por exemplo, pode se tratar de preparar as saídas sobre suporte de papel ou transferir os dados para outro sistema.

Nenhum dado armazenado eletronicamente pode ser destruído sem a previa autorização da gerência e sem a aplicação da documentação adequada. Os demais dados auxiliares relativos aos sistemas informatizados, como por exemplo os códigos-fonte e os arquivos de desenvolvimento, de validação, de operação, de manutenção e de controle devem ser conservados durante, no mínimo o mesmo período de tempo que os registros e os estudos associados a estes sistemas.

DEFINIÇÃO DOS TERMOS

Assinatura eletrônica: entrada, em forma de impulsos magnéticos ou de dados informatizados adquiridos, de qualquer símbolo ou conjunto de símbolos, executada, adaptada ou autorizada por uma pessoa para representar sua assinatura manuscrita.

Back-up: Disposições projetadas para recuperar os arquivos de dados ou softwares, iniciar novamente o processamento ou utilizar os equipamentos informatizados de substituição no caso de falha do sistema ou acidente.

Código-fonte: Programa informatizado originalmente redigido em uma linguagem legível pelo homem (linguagem de programação) que se traduz para a linguagem de máquina antes de poder ser executada pelo computador.

Controle das alterações: Avaliação permanente tomando como fundamento os documentos justificados das operações executadas por um sistema e de sua modificação para determinar se é necessário aplicar um procedimento de validação através de qualquer modificação do sistema informatizado.

Critérios de aceitação: Critérios definidos e documentados que devem ser seguidos para concluir positivamente a fase de testes ou ensaios, ou considerar que o sistema atende as exigências.

Hardware: Conjunto de elementos físicos de um sistema informatizado que inclui a unidade central do computador e seus periféricos.

Normas técnicas reconhecidas: Normas promulgadas por organismos nacionais ou internacionais de normalização (ISO, IEEE, ANSI, etc).

Periférico: Qualquer equipamento conectado com um sistema ou elemento auxiliar ou a distância, como por exemplo: impressoras, placa de modem, terminais, etc.

Software (aplicativo): Um programa incorporado ou desenvolvido, adaptado ou personalizado em função das condições da Unidade Operacional, para garantir os procedimentos de controle, coleta, processamento, apresentação e/ou arquivo dos dados.

Software (sistema operacional): Programa, conjunto de programas ou de subprogramas que governam o funcionamento do computador. Um sistema operacional pode executar as tarefas como alocação de recursos, agendamento, gestão das entradas / saídas e gestão dos dados.

Segurança: Proteção do hardware e do software contra o acesso, a utilização, a modificação, a destruição ou a divulgação, acidentais ou intencionais. A segurança aplica-se também ao pessoal, aos dados, às comunicações e a proteção física e lógica das instalações informáticas.

Sistema informatizado: Grupo de elementos do equipamento (hardware), acompanhado dos softwares correspondentes, projetado e reunido para permitir uma função ou um grupo de funções determinadas.

Teste de recepção: Teste formal de um sistema informatizado no contexto operacional projetado para verificar se todos os critérios da Unidade Operacional foram devidamente respeitados e se o sistema pode ser aceito para funcionar no modo operacional.

Validação de um sistema informatizado: Operação que permite demostrar que um sistema informatizado corresponde perfeitamente às tarefas para as quais está destinado.